[info]

**Introduction**

ServMon est un Windows dont l’adresse IP est 10.10.10.184.

Compétences mises en œuvre :

* Enumération des ports et services.
* Vérification FTP
* Identification d’un service web vulnérable.
* Recherche et exploitation de CVE (LFI).
* Enumération des services Windows.
* Redirection de port (port forwarding sous SSH) sous Windows.

**Enumération initiale**

Nous commençons comme toujours par l’énumération des ports et services de la machine avec nmap :

|  |
| --- |
| $ nmap -T4 -A 10.10.10.184 |

[nmap]

Plusieurs ports ouverts, nous allons commencer par énumérer les fichiers/dossiers accessible sur le FTP puis nous passerons à l’énumération des sites web.

|  |
| --- |
| $ ftp |

[ftp]

Maintenant les serveurs web, étant donné qu’il y en a deux, nous allons nous attarder sur le sécurisé (port 443) avec une énumération de dossier/fichier avec dirsearch :

|  |
| --- |
| $ dirsearch |

[dirsearch]

En attendant la fin d’ énumération, nous allons effectuer un rapide tour sur l’interface web, nous pouvons voir que la technologie utilisée est : NVMS-100 . Nous allons donc rechercher une CVE ou un exploit concernant NVMS avec searchsploit et google :

|  |
| --- |
| $searchsploit NVMS |

[searchsploit]

**Obtenir un accès utilisateur**

Bla

**Obtenir un accès root**

Bla